RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: PNG-T10

A Year(ish) of Countering Malicious Actors' Use of AI: What Have We Learned?

MODERATOR: **Cynthia Kaiser**
Deputy Assistant Director, FBI Cyber

PANELISTS: **Lyn Brown**
Partner
Wiley Rein LLP

Sherrod DeGrippo
Director of Threat Intelligence Strategy
Microsoft

Adam Maruyama
Field CTO for Digital Transformation and AI
Everfox

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

The material contained in this presentation from Wiley Rein LLP is for informational purposes only. It is not intended to be and is not considered to be legal advice. Legal advice of any nature should be sought from legal counsel.

Applicable panel participants are providing their personal opinions and experience as current or former US Government employees and not the official position of the federal government.

RSAC 2025 Conference

#RSAC

Many Voices.
One Community.

MODERATOR:

Cynthia Kaiser

Deputy Assistant Director
FBI Cyber

cynthia-kaiser-cyber

PANELISTS:

Lyn Brown

Partner
Wiley Rein LLP

lyn-brown-52a72a9

Sherrod DeGrippo

Director of Threat Intelligence Strategy
Microsoft

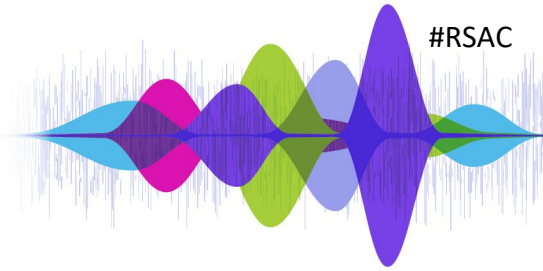
sherroddigrippo

Adam Maruyama

Field CTO for Digital Transformation and AI
Everfox

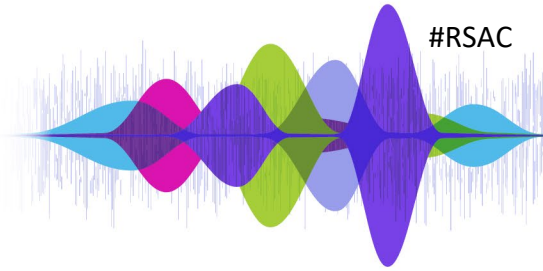
adam-maruyama

Countering Malicious Actors' Use of AI: What Have We Learned?



- **Lesson #1:** **Adversaries are more efficient, and trying to do more**

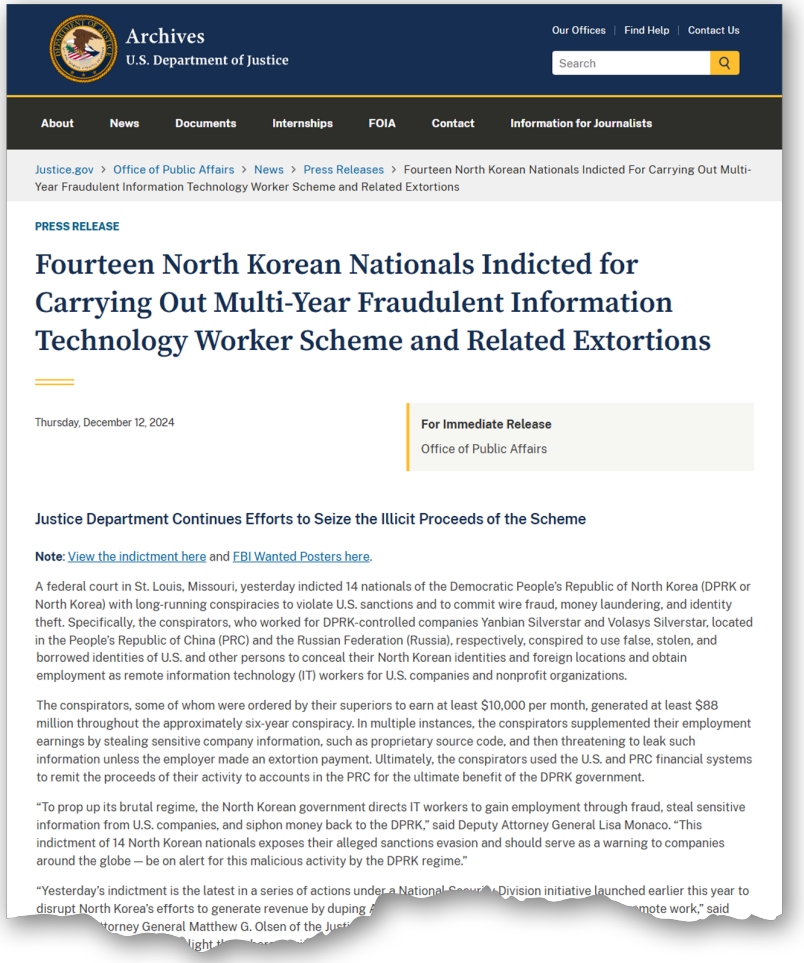
Countering Malicious Actors' Use of AI: What Have We Learned?



- Lesson #1: Adversaries are more efficient, and trying to do more
- Lesson #2: **Same laws, new stories**

Disrupting Malicious Operations Using AI

US Government Disrupts North Korean IT Workers Scheme



Archives
U.S. Department of Justice

Our Offices | Find Help | Contact Us

Search

About | News | Documents | Internships | FOIA | Contact | Information for Journalists

Justice.gov > Office of Public Affairs > News > Press Releases > Fourteen North Korean Nationals Indicted For Carrying Out Multi-Year Fraudulent Information Technology Worker Scheme and Related Extortions

PRESS RELEASE

Fourteen North Korean Nationals Indicted for Carrying Out Multi-Year Fraudulent Information Technology Worker Scheme and Related Extortions

Thursday, December 12, 2024

For Immediate Release
Office of Public Affairs

Justice Department Continues Efforts to Seize the Illicit Proceeds of the Scheme

Note: View the indictment here and FBI Wanted Posters here.

A federal court in St. Louis, Missouri, yesterday indicted 14 nationals of the Democratic People's Republic of North Korea (DPRK or North Korea) with long-running conspiracies to violate U.S. sanctions and to commit wire fraud, money laundering, and identity theft. Specifically, the conspirators, who worked for DPRK-controlled companies Yanbian Silverstar and Volasys Silverstar, located in the People's Republic of China (PRC) and the Russian Federation (Russia), respectively, conspired to use false, stolen, and borrowed identities of U.S. and other persons to conceal their North Korean identities and foreign locations and obtain employment as remote information technology (IT) workers for U.S. companies and nonprofit organizations.

The conspirators, some of whom were ordered by their superiors to earn at least $10,000 per month, generated at least $88 million throughout the approximately six-year conspiracy. In multiple instances, the conspirators supplemented their employment earnings by stealing sensitive company information, such as proprietary source code, and then threatening to leak such information unless the employer made an extortion payment. Ultimately, the conspirators used the U.S. and PRC financial systems to remit the proceeds of their activity to accounts in the PRC for the ultimate benefit of the DPRK government.

"To prop up its brutal regime, the North Korean government directs IT workers to gain employment through fraud, steal sensitive information from U.S. companies, and siphon money back to the DPRK," said Deputy Attorney General Lisa Monaco. "This indictment of 14 North Korean nationals exposes their alleged sanctions evasion and should serve as a warning to companies around the globe — be on alert for this malicious activity by the DPRK regime."

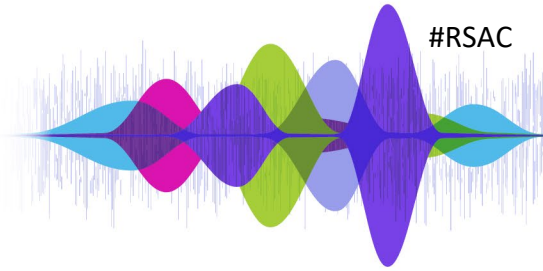
"Yesterday's indictment is the latest in a series of actions under a National Security Division initiative launched earlier this year to disrupt North Korea's efforts to generate revenue by duping [illegible] remote work," said [illegible] Attorney General Matthew G. Olsen of the Justi[illegible]

Disrupting a global cybercrime network abusing generative AI

Feb 27, 2025 | Steven Masada - Assistant General Counsel, Microsoft's Digital Crimes Unit

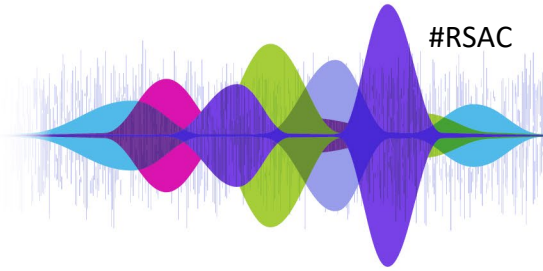
Microsoft Disrupts Storm-2139 Global Cybercrime Network

Countering Malicious Actors' Use of AI: What Have We Learned?



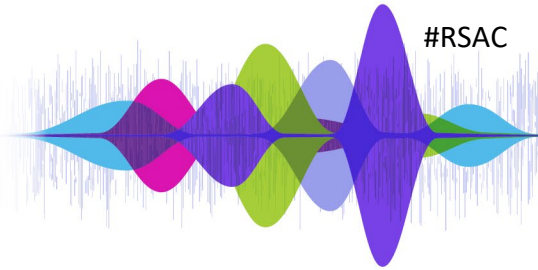
- Lesson #1: Adversaries are more efficient, and trying to do more
- Lesson #2: Same laws, new stories
- **Lesson #3: There are still a lot of operational unknowns**

Countering Malicious Actors' Use of AI: What Have We Learned?



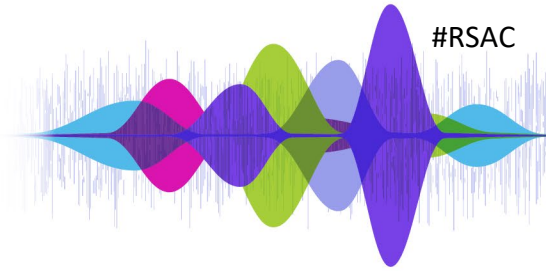
- Lesson #1: Adversaries are more efficient, and trying to do more
- Lesson #2: Same laws, new stories
- Lesson #3: There are still a lot of operational unknowns
- **Lesson #4: Benefits weighed toward cybersecurity**

Hardening Our Defenses



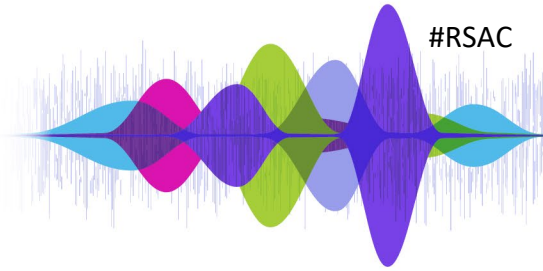
- **Protect Your Company and Yourself**
  - Know AI models in your environment (Software Bill of Materials for AI)
  - Integrate AI threat detection and security applications
  - Include deterministic technologies like Remote Browser Isolation (RBI) and hardware-enforced security (hardsec) in your Zero Trust model
  - Authenticate people and content (MFA/C2PA)
  - Implement deepfake detection strategies, like these FBI tips
- **Strengthen Relationships between Government and Industry**
  - We all need to work together to counter these new threats

Countering Malicious Actors' Use of AI: What Have We Learned?



- Lesson #1: Adversaries are more efficient, and trying to do more
- Lesson #2: Same laws, new stories
- Lesson #3: There are still a lot of operational unknowns
- Lesson #4: Benefits weighed toward cybersecurity
- **Lesson #5: We can make progress against these threats**

Countering Malicious Actors' Use of AI: What Have We Learned?



- **Lesson #1:** Adversaries are more efficient, and trying to do more
- **Lesson #2:** Same laws, new stories
- **Lesson #3:** There are still a lot of operational unknowns
- **Lesson #4:** Benefits weighed toward cybersecurity
- **Lesson #5:** We can make progress against these threats

RSAC™ 2025 Conference

Together, we can make progress against these threats

Many Voices.
One Community.